

如何指定 TACACS+ 和 RADIUS 的权限级别

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[示例](#)

[配置 - 路由器](#)

[配置 - 服务器](#)

[相关信息](#)

简介

本文档介绍如何更改特定命令的权限级别，并提供适用于路由器与 TACACS+ 和 RADIUS 服务器的部分示例配置。

先决条件

要求

本文档的读者应具备路由器权限级别知识。

默认情况下，路由器上有三个权限级别。

- 权限级别 1 = 无特权（提示符是 `router>`），这是登录的默认级别
- 权限级别 15 = 有特权（提示符是 `router#`），这是进入启用模式后的级别
- 权限级别 0 = 很少使用，但包括 5 个命令：**disable**、**enable**、**exit**、**help** 和 **logout**

级别 2-14 不在默认配置中使用，但级别 15 的常见命令可以下调至这些级别的其中一个，而级别 1 的常见命令也可以上调至这些级别的其中一个。显然，此安全模式涉及路由器上的某些管理。

要以登录用户身份确定权限级别，请键入 **show privilege** 命令。要确定特殊权限级别的哪些命令适用于您正使用的 Cisco IOS® 软件版本，请在以该权限级别登录时，在命令行中键入 **?**。

注意：如果认证服务器支持 TACACS+，您将能够执行命令授权，而不用分配权限级别。RADIUS 协议不支持命令授权。

使用的组件

本文档中的信息基于 Cisco IOS 软件版本 11.2 及以上。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[示例](#)

在本示例中，**snmp-server** 命令从权限级别 15（默认）下调至权限级别 7。**ping** 命令从权限级别 1 上调至权限级别 7。当验证用户 seven 时，服务器将对该用户分配权限级别 7，并且发出 **show privilege** 命令将显示“Current privilege level is 7”。用户可以执行 ping 操作并在配置模式下执行 snmp-server 配置。其他配置命令不可用。

[配置 - 路由器](#)

[路由器 - 11.2](#)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

[路由器 - 11.3.3.T 及以上 \(直至 12.0.5.T\)](#)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

[路由器 - 12.0.5.T 及以上](#)

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
```

```
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

[配置 - 服务器](#)

[Cisco Secure NT TACACS+](#)

按照以下步骤配置服务器。

1. 填写用户名和口令。
2. 在 Group Settings 中，确保选中 shell/exec，并且已将 7 输入 privilege level 框中。

[TACACS+ -在免费软件服务器的Stanza](#)

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

[Cisco Secure UNIX TACACS+](#)

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

[Cisco Secure NT RADIUS](#)

按照以下步骤配置服务器。

1. 输入用户名和口令。
2. 在 Group Settings for IETF 中，Service-type (属性 6) = Nas-Prompt

3. 在 CiscoRADIUS 区域中，选中 **AV-Pair**，并在下面的矩形框中输入 **shell:priv-lvl=7**。

Cisco Secure UNIX RADIUS

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

这是用户名“seven”的用户文件。

注意： 服务器必须支持 Cisco av-pairs。

- seven Password = **passwdxyz**
- Service-Type = **Shell-User**
- cisco-avpair =**shell:priv-lvl=7**

相关信息

- [RADIUS 支持页](#)
- [请求注解 \(RFC\)](#)
- [IOS 文档中的 TACACS+](#)
- [TACACS+ 支持页](#)
- [Cisco Secure UNIX 支持页](#)
- [Cisco Secure ACS for Windows 支持页](#)
- [技术支持 - Cisco Systems](#)